依循作業流程步驟，順利處理資安事件，於最短時間內完成復原。

如何建立資安事件應變程序

◎張嘉哲

壹、緒論

行政院國家資通安全會報於93年10月即已頒訂「各機關（構）落實資安事件危機處理具體執行方案」，規範「資安事件通報與應變作業流程」。該流程主要著重於通報程序管制要求，但對於特定之資安事件，如網頁置換攻擊、入侵事件及異常網路連線等，仍欠缺更明確與可遵循之應變作業程序。

為協助政府機關落實有效之資安事件應變處理程序，並在發生資安事件時，能迅速進行正確的緊急應變處置，於最短時間內完成復原。本文將以國家資通安全會報技術服務中心（以下簡稱技服中心）所發布的資安警訊「入侵事件警訊—對外攻擊」為例，建立相對應之資安事件應變程序。

貳、資安事件應變程序生命週期

由於要有效地執行資安事件應變是一件複雜的工作，因此需事先規劃符合組織或企業內部的資安事件應變程序，即成為相當重要的根基。根據美國國家標準與技術局（National Institute of Standards and Technology, NIST）所出版的一份「Computer Security Incident Handling Guide」文件中指出，資安事件應變程序的生命週期應包含四個階段：「準備（Preparation）」、「偵測與分析（Detection and Analysis）」、「封鎖、移除與回復（Containment, Eradication, and Recovery）」，以及「事後處理（Post-Incident Activity）」，詳見圖１，並分別說明如下：

資料來源：NIST，http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51289　圖1　資安事件應變程序生命週期

一、準備階段（Preparation）

正如孫子兵法所云：「知己知彼，百戰百勝」，組織或企業資訊人員平時應多增加資訊安全相關知識，清楚各類型的資安風險與威脅，了解若未落實資安防護工作，則資安事件可能伴隨而來。因此平日的資安防護準備工作相當重要，例如：作業系統與常用軟體版本更新機制、帳號與密碼更新管理、資安防護設備部署作業或使用者資安認知訓練、規劃災害復原計畫等，均能減少資安事件的發生機率，並降低遭逢資安事件衝擊所受到的風險。

二、偵測與分析階段（Detection and Analysis）

透過資安設備的部署，以及建立相對應的資安防護機制後，即開始進行偵測潛在性的資訊安全事件。此階段主要可透過各類型的資安設備進行偵測，或藉由專業人員觀察所發現，並可由以下方式進行判斷，分析是否確實可能造成資訊安全事件的產生：

1. 前兆（Precursors）
   現階段並不會出現立即性的症狀，但有可能未來即將發生資安事件，例如：檢視網站日誌檔發現有駭客進行網頁弱點掃描，或是接獲駭客恐嚇，宣稱將攻擊網站伺服器等。
2. 症狀（Indications）
   資安事件可能為立即性或正在發生當中，例如：觸發入侵偵測系統的規則、防毒軟體偵測到惡意程式、網站伺服器無法存取、使用者抱怨網路速度過慢、網站頁面遭到竄改等。

三、封鎖、移除與回復階段（Containment, Eradication, and Recovery）

經確認資安事件發生後，應立即採取合適的應變工作，例如確保各種日誌的保存，透過分析日誌，確定攻擊來源IP，並加以封鎖，經由事先建立的災害復原計畫進行回復作業，確保組織或企業的系統或服務能迅速恢復運作。

四、事後處理階段（Post-Incident Activity）

由於資安設備並非萬能，亦沒有所謂100%安全的系統，會發生資安事件必定在資安防護上有所缺失，透過事後處理階段可檢視資安事件發生的原因，可能是系統安全設定不良，或是資安管理政策上有所不足，甚至是人為或天災因素所造成。若能釐清事件發生原因並加以改善，進而加強準備階段工作，則可避免相同資安事件再次發生。

參、定義資安事件

在NIST撰寫「Computer Security Incident Handling Guide」文件中定義了各種不同的資安事件類型，其中包含阻斷服務（Denial of Service）、惡意程式（Malicious Code）、非法存取（Unauthorized Access），以及不當使用（Inappropriate Usage），因此組織或企業於資安事件應變程序生命週期的準備階段時，建議應事先自行定義資安事件種類，不同的資安事件應有相對應之應變程序。

技服中心對於各類型資安事件均有詳加定義，同時搭配資安訊息發布服務，提供政府機關適當的資訊，協助及早發現並處理潛在的資安威脅，降低因資安事件所造成的損失。技服中心目前對外共發布５大類資安事件警訊，分別為：資安預警警訊、入侵事件警訊、網頁攻擊警訊、資安訊息警訊，以及緊急事件警訊。

其中「入侵事件警訊—對外攻擊」的資安事件定義，若政府機關的資訊設備遭受駭客入侵後，可能會成為跳板或殭屍電腦（Bot），進而攻擊或嘗試入侵其他主機。一旦經技服中心確認是攻擊行為並判定為資安事件，將會發布此類型之入侵事件警訊，同時通知政府機關的資安聯絡人，請其進行資安事件通報與處理。

肆、建立資安事件應變程序

本文將資安事件應變程序生命週期歸納成兩個部分，分別為「資安事件發生前之預防」與「資安事件發生後之處理」。「資安事件發生前之預防」包含了資安事件應變程序生命週期的前兩個階段，即「準備階段」和「偵測與分析階段」；「資安事件發生後之處理」則涵蓋後兩個階段，即「封鎖、移除與回復階段」和「事後處理階段」。

「資安事件發生前之預防」需仰賴提升組織或企業人員的資安素養並加強平日資安防護的準備工作；而技服中心所制定之資安事件應變程序乃著重在「資安事件發生後之處理」，一旦經由技服中心發布資安警訊予政府機關，或是由政府機關自行發現資安事件時，能透過步驟化的方式，提供人員順利蒐集受駭資訊設備的基本資訊，以進行後續的通報作業與採取相關應變措施等工作。以下將以「入侵事件警訊－對外攻擊」的資安事件為例，建立相對應之應變程序，主要分成５個步驟，分別說明如下：

一、【STEP 1】確認受駭資訊設備

由於駭客在入侵資訊設備後，可能會進行對外攻擊行為，因此當政府機關資安聯絡人員接獲由技服中心發送入侵事件警訊，而其事件類型為對外攻擊時，建議先行確認受駭資訊設備，並蒐集受駭資訊設備之基本資訊，內容應包含實體主機IP位址、設備廠牌與機型、網際網路位址、作業系統名稱與版本，以及已裝置之安全機制。

二、【STEP 2】執行通報程序

因入侵事件警訊已由技服中心判定為確切之資安事件，一旦政府機關接獲此類警訊，並完成蒐集受駭資訊設備之基本資訊後，政府機關人員應依循「國家資通安全會報通報應變流程」執行通報程序，包含內部通報作業及至國家資通安全通報應變網站辦理通報，提供事件細節、影響等級和支援申請項目等資訊，並陸續回報後續資安事件處理情形。

三、【STEP 3】判斷與應變措施

完成執行通報程序後，需立即採取相對的緊急應變措施，建議包含下列工作：

1. 判斷是否需中斷受駭資訊設備的連線行為，其目的為避免機敏資料洩漏，減少因資安事件所造成之損害程度。
2. 判斷是否需停止網路服務，若受駭資訊設備提供網路服務，如：網站伺服器（Web Server）或郵件伺服器（Mail Server）等，其目的為縮小因資安事件所造成之受駭範圍。
3. 確認資訊設備的破壞程度，受駭資訊設備可能在駭客入侵或植入惡意程式後出現異常的網路連線情形，政府機關人員需確認其造成的破壞程度，例如：系統當機、資料庫毀損或網頁遭竄改等。
4. 判斷資安事件影響等級，依據「國家資通安全會報通報應變流程」規定，需判斷資安事件影響等級，由輕至重分為「１」、「２」、「３」及「４」個級別，並以該事件造成對資訊「機密性」、「完整性」及「可用性」的衝擊，綜合評估該事件的影響等級。

四、【STEP 4】釐清事件發生原因

每個資安事件的發生，其背後一定有特定的原因，政府機關人員可能需透過分析各種日誌檔，例如：網站伺服器、防火牆、DNS伺服器、電子郵件伺服器、系統錯誤訊息，或是檢查使用者的受駭資訊設備，進而找出資安事件發生的原因，例如：惡意程式、系統設定錯誤、應用程式弱點、人為因素等。

在分析與釐清資安事件發生原因時，若政府機關人員遇到技術上的困難或問題，建議先向協力廠商尋求支援，請其調查事件發生原因與提供解決方案。若協力廠商亦無法釐清事件發生原因時，可透過國家資通安全通報應變網站向技服中心提出技術支援申請，並記錄期望的支援項目，由主管機關與技服中心審核該等支援項目是否可協助處理。

五、【STEP 5】參考復原建議

分析資安事件發生的原因後，應依事先準備的災害復原計畫進行回復作業。依據「國家資通安全會報通報應變流程」之事件影響等級，若通報事件影響等級為３、４級，需於事件後36小時內復原或完成損害管制作業；１、２級則需於72小時內復原或完成損害管制作業。

鑒於入侵事件警訊內容顯示受駭資訊設備確實有對外攻擊情形，研判資訊設備已遭駭客入侵並加以控制，政府機關人員除可尋求協力廠商提供復原建議外，亦可參閱技服中心提供之警訊防護建議措施與參考資料，依不同的資訊安全政策選擇合適的復原與防護措施，並記錄相關復原方式，例如：還原系統、重新安裝作業系統或安裝修補程式等。

此外，當政府機關人員完成災害復原或損害管制作業後，須至國家資通安全通報應變網站進行通報結案，說明資安事件之後續處理情形與追蹤事項，並記錄完成結案日期。

由上述5個步驟可知，技服中心對於「資安事件發生後之處理」定義較詳細的步驟與說明，其中STEP 1至STEP 3在資安事件應變程序生命週期中屬於「封鎖、移除與回復階段」，STEP 4至STEP 5則屬於「事後處理階段」。各組織可自行定義不同的資安事件，並建立合適的資安事件應變程序，期能迅速完成復原，降低資安事件造成的損害。

伍、結語

發生資安事件時，為了能採取緊急應變措施，並迅速恢復系統運作與服務提供，因此需事先定義資安事件應變程序。企業或組織均可參考美國國家標準與技術局（NIST）所制定之資安事件應變程序生命週期，各自發展合適的資安事件應變流程。

本文將資安事件應變程序的生命週期歸納成兩個部分，分別為「資安事件發生前之預防」與「資安事件發生後之處理」，並以技服中心所制定的資安事件「入侵事件警訊—對外攻擊」為例，著重在「資安事件發生後之處理」，建立符合國家資通安全通報應變綱要規定之應變程序。透過步驟化的方式說明執行內容，可協助政府機關人員了解接獲資安警訊通知後的處置措施。政府機關人員在接獲資安警訊通知時，僅需依循作業流程步驟，即可順利處理資安事件。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心副工程師）

▲Top